

## EXHIBIT 4

1 KEKER & VAN NEST, LLP  
JOHN W. KEKER - #49092  
2 MICHAEL H. PAGE - #154913  
710 Sansome Street  
3 San Francisco, CA 94111-1704  
Telephone: (415) 391-5400  
4 Facsimile: (415) 397-7188

5 DERWIN & SIEGEL, LLP  
DOUGLAS K. DERWIN - #111407  
6 3280 Alpine Road  
Portola Valley, CA 94028  
7 Telephone: (408) 855-8700  
Facsimile: (408) 529-8799

8 INTERTRUST TECHNOLOGIES CORPORATION  
9 JEFFERY J. McDOW - #184727  
4800 Patrick Henry Drive  
10 Santa Clara, CA 95054  
Telephone: (408) 855-0100  
11 Facsimile: (408) 855-0144

12 Attorneys for Plaintiff and Counter-Defendant  
INTERTRUST TECHNOLOGIES CORPORATION  
13

14 UNITED STATES DISTRICT COURT  
15 NORTHERN DISTRICT OF CALIFORNIA  
16

17 INTERTRUST TECHNOLOGIES  
CORPORATION, a Delaware corporation,  
18  
19 Plaintiff,

20 v.

21 MICROSOFT CORPORATION, a  
Washington corporation,  
22 Defendant.

Case No. C 01-1640 SBA (MEJ)

Consolidated with C 02-0647 SBA

**PLAINTIFF INTERTRUST  
TECHNOLOGIES CORPORATION'S  
REPLY MEMORANDUM ON CLAIM  
CONSTRUCTION**

Date: May 12, 29, & 30, 2003

Time: 9:00 a.m.

23 AND COUNTER ACTION.  
24  
25  
26  
27  
28

# TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION .....	1
II. ARGUMENT .....	2
A. Microsoft's Requirement of Absolute, "True" Security Contradicts the Specification. ....	2
1. Microsoft's VDE construction requires that the claims be interpreted to require an extremely high degree of security. ....	2
2. The specification discloses embodiments that do not require the highest degree of security. ....	3
3. The patent claims do not specify a high degree of security. ....	4
4. Microsoft's massive definition of "secure" invites the Court to usurp the jury's role in conducting the infringement analysis. ....	4
B. Microsoft's VDE-Based Interpretation Requires Excluding Disclosed Embodiments. ....	5
1. Tamper-Resistant Barrier. ....	5
2. Protected processing environment. ....	6
C. Microsoft's Legal Arguments Are Misleading. ....	7
D. Microsoft's Argument that the Claims Require VDE is Wrong. ....	7
1. '193 patent claims. ....	7
2. '683, claim 2. ....	11
3. '721, Claims 1 and 34. ....	11
4. Other claims. ....	12
E. Microsoft's Bases for Reading the Specification Into the Claims Are Either Mischaracterized or Do Not Apply. ....	12
F. Microsoft's Argument about the InterTrust Divisionals Misses the Point. ....	15
G. Individual Claim Elements. ....	16
1. Microsoft ignores ten claim elements. ....	16
2. Use. ....	17
3. Copy. ....	17

**TABLE OF CONTENTS**  
**(cont'd)**

	<u>Page</u>
4. Secure/Securely.....	17
5. Secure Container.....	18
6. Tamper Resistant Barrier.....	19
7. Protected Processing Environment.....	20
8. Component Assembly.....	20
9. Control (noun).....	21
10. A budget specifying the number of copies which can be made of said digital file (193.1).....	22
11. Container.....	22
12. Containing.....	22
13. Control (verb) / Controlling.....	22
14. "Controlling the copies made of said digital file" (193.1).....	22
15. "Derives information from one or more aspects of said host processing environment" (900.155).....	23
16. Host Processing Environment.....	23
17. Identifier.....	23
18. Tamper Resistance.....	24
19. Budget.....	24
20. Clearinghouse.....	24
H. Testimony Cited by Microsoft.....	25
III. CONCLUSION.....	25

## TABLE OF AUTHORITIES

Page(s)

### Federal Cases

<u>Altiris, Inc. v. Symantec Corp.</u> , 318 F.3d 1363 (Fed. Cir. 2003) .....	12
<u>Ballard Med. Prod. v. Allegiance Healthcare Corp.</u> , 268 F.3d 1352 (Fed. Cir. 2001) .....	16
<u>CCS Fitness, Inc. v. Brunswick Corp.</u> , 288 F.3d 1359 (Fed. Cir. 2002) .....	14
<u>Ethicon Endo-Surgery v. United States Surgical Corp.</u> , 93 F.3d 1572 (Fed. Cir. 1996) .....	13
<u>Gerber Garment Tech., Inc. v. Lectra Sys. Inc.</u> , 916 F.2d 683 (Fed. Cir. 1990) .....	15, 16
<u>Innovad, Inc. v. Microsoft</u> , 260 F.3d 1326 (Fed. Cir. 2001) .....	14
<u>Inverness Med. Switz. GmbH v. Princeton Biomeditech Corp.</u> , 309 F.3d 1365 (Fed. Cir. 2002) .....	17
<u>Johns Hopkins Univ. v. CellPro, Inc.</u> , 152 F.3d 1342 (Fed. Cir. 1998) .....	5
<u>Markman v. Westview Instruments, Inc.</u> , 52 F.3d 967, <u>aff'd</u> , 517 U.S. 370 (1996) .....	8, 19, 22, 25
<u>Modine Mfg. Co. v. United States Int'l Trade Comm.</u> , 75 F.3d 1545, 37 U.S.P.Q.2D (BNA) 1609 (Fed. Cir. 1996) .....	5
<u>NeoMagic Corp. v. Trident Microsystems, Inc.</u> , 287 F.3d 1062 (Fed. Cir. 2002) .....	13
<u>North Am. Vaccine v. American Cyanamid Co.</u> , 7 F.3d 1571 (Fed. Cir. 1993) .....	13
<u>PPG Indus., Inc. v. Guardian Indus. Corp.</u> , 156 F.3d 1351 (Fed. Cir. 1998) .....	5, 20
<u>Rheox, Inc. v. Entact, Inc.</u> , 276 F.3d 1319 (Fed. Cir. 2002) .....	14
<u>SciMed Life Sys. v. Advanced Cardiovascular Sys.</u> , 242 F.3d 1337 (Fed. Cir. 2001) .....	13, 14
<u>Spectrum Int'l v. Sterilite Corp.</u> , 164 F.3d 1372 (Fed. Cir. 1998) .....	14
<u>Toro Co. v. White Consol. Indus.</u> , 199 F.3d 1295 (Fed. Cir. 1999) .....	14
<u>Watts v. XL Sys., Inc.</u> , 232 F.3d 877 (Fed. Cir. 2000) .....	13

### Statutes

35 U.S.C. § 112(6) .....	16
--------------------------	----

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

TABLE OF AUTHORITIES  
(cont'd)

Page(s)

**Other Authorities**

American Heritage Dictionary..... 23

1  
2 I. INTRODUCTION

3 Microsoft's claim construction positions derive from a single underlying premise: the  
4 details of the "VDE" embodiment described in the specifications must be read into every claim,  
5 and every claim element must be interpreted so as to include all of the VDE limitations.  
6 According to Microsoft, this is so because the patents "promise" an extremely high degree of  
7 security ("truly secure") that Microsoft alleges can only be supplied by the VDE embodiment.

8 Microsoft acknowledges, however, that the patents describe varying levels of security,  
9 ranging from the extremely high degree of security provided by the "truly secure" embodiment  
10 to much lower levels of security. The patents refer to all of these levels of security as "secure,"  
11 and each of them represents a degree of security appropriate to particular circumstances.  
12 Microsoft's constructions exclude all levels of security other than the extremely high "truly  
13 secure," not because the claims specify this high level of security (they are silent regarding the  
14 particular level of security required and do not mention "true" security), not because the  
15 specification requires such an interpretation (it describes varying degrees of security) and not  
16 because the ordinary meaning of the claim terms requires such an interpretation (Microsoft  
17 acknowledges its definition of "secure" is not standard).

18 Instead, Microsoft excludes all levels of security other than the highest possible level  
19 because, according to Microsoft, only the highest possible level is consistent with the "VDE  
20 invention." Microsoft contends that lower security embodiments should be ignored during claim  
21 construction, because in some places the specification uses the word "invention" in combination  
22 with VDE, thereby allegedly requiring that 115 pages, including "literally hundreds" of  
23 limitations, be read into every claim.

24 Microsoft's requirement that the "VDE invention" be imported into every claim leads  
25 Microsoft to claim constructions that directly contradict the definition given to the same terms in  
26 the specification. For example, the specification describes two embodiments of "tamper resistant  
27 barrier," a higher-security hardware embodiment and a lower-security software embodiment.  
28 Both of these embodiments are identified in the specification as a "tamper resistant barrier."  
Microsoft, however, demands that the claim term "tamper resistant barrier" be defined to exclude

1 the software embodiment, since the software embodiment is inconsistent with Microsoft's  
2 requirement that VDE "true security" be read into every claim. Similarly, the specification  
3 describes two embodiments of "protected processing environment," a higher-security hardware  
4 embodiment and a lower-security software embodiment, both identified in the specification as a  
5 "protected processing environment." Microsoft's construction of "protected processing  
6 environment" excludes the software embodiment, again because this is inconsistent with  
7 Microsoft's requirement that VDE "true security" be read into every claim element.

8 The Federal Circuit has held that claim constructions that exclude disclosed embodiments  
9 are "rarely, if ever" correct. Microsoft's "VDE invention" construction of the claims ignores  
10 specification embodiments describing levels of security different than extremely secure "true"  
11 security, and contradicts the specification's use of the claim terms. Microsoft's construction  
12 must therefore be rejected as being inconsistent with the patent specifications.

## 13 II. ARGUMENT

### 14 A. Microsoft's Requirement of Absolute, "True" Security Contradicts the 15 Specification.

#### 16 1. Microsoft's VDE construction requires that the claims be interpreted to 17 require an extremely high degree of security.

18 Microsoft's proposed constructions require that "each type of property identified in the  
19 patents is 'truly secure' against all types and levels of threats identified in the patents." MS Br.,  
20 28:1-2. According to Microsoft, this requires that "all users" are "guaranteed that all  
21 information, processes, and devices" will have five separate properties "maintained against all of  
22 the identified threats thereto." MS Br., 28:2-5. Microsoft justifies this extreme position by  
23 arguing that none of the patents excludes what Microsoft characterizes as "true security." MS  
24 Br., 28:7-17. Thus, Microsoft's brief includes statements such as the following:

25 [T]he Big Book promises "true" security. It promises the ability to "prevent"  
26 unauthorized uses, etc., and "ensure" that rights will be enforced, and "guarantee"  
trustworthiness, even when faced with strong, sophisticated attacks against high-  
value content. Nothing in the claims indicates an inability to live up to these  
promises and protect such high-value content against such strong attacks.

27 MS Br., 32:16-20 (emphasis added). See also Id., 3:4-11, 17:4-6.



1 Microsoft asks that claims be interpreted narrowly so as to exclude all levels of security  
2 other than this "true" security, security so high as to amount to an absolute "guarantee" of  
3 protection against all threats, "no matter what effort may be made" to break the protection.

4 **2. The specification discloses embodiments that do not require the highest**  
5 **degree of security.**

6 As Microsoft acknowledges, the patents describe a variety of levels of security. Thus,  
7 Microsoft states that the patents use "secure" "to mean different things in different places," (MS  
8 Br., 25:18-19), and "the term 'secure' is used in the specification to refer to different things in  
9 different contexts." MS Br., 27:10-11.

10 The passage Microsoft relies upon for its requirement of "true" security makes exactly  
11 this point:

12 The SPU 502 may be used to perform all **truly secure** processing, whereas one or  
13 more HPEs 655 may be used to provide **additional secure (albeit possibly less**  
**secure than the SPE) processing . . . Any service may be provided by such a**  
**secure HPE . . . .**

14 '193 patent, 80:30-36 (JCCS Ex. C, 22(B) (emphasis added).

15 Other passages similarly indicate that different degrees of protection may be desirable in  
16 different contexts:

17 Because security may be better/more effectively enforced with the assistance of  
18 hardware security features such as those provided by SPU 500 (and because of  
19 other factors such as increased performance provided by special purpose circuitry  
20 within SPU 500), **at least one SPE 503 is preferred for many or most higher**  
**security applications. However, in applications where lesser security can be**  
**tolerated and/or the cost of an SPU 500 cannot be tolerated, the SPE 503 may be**  
**omitted and all secure processing may instead be performed by one or more**  
**secure HPEs 655 executing on general-purpose CPUs 654.**

21 '193 patent at 80:65-81:8 (JCCS Ex. C, 19(N)) (emphasis added). Additional examples  
22 of specification passages describing security levels below the highest level are found at JCCS  
23 Ex. C, 19(B), (C), (J), and (M).

24 Thus, the parties agree that the patent specification describes different degrees of  
25 security, including "truly" secure and "less" secure. The word "secure" is used to refer to both  
26 of these levels.  
27  
28

1           **3. The patent claims do not specify a high degree of security.**

2           The claims do not require “true” security. Both disclosed embodiments (truly secure and  
3 less secure) are within the scope of the word “secure” as used in the specification.

4           That “secure” is used to refer to different levels and degrees of security supports  
5 InterTrust’s definition, since that definition allows such different degrees. Microsoft, however,  
6 argues that the breadth given to the term in the specification actually supports reading the most  
7 extreme disclosed embodiment into the claims, on the theory that the claims do not “exclude”  
8 this embodiment. MS Br., 28:12-13.<sup>1</sup> Microsoft further alleges that the context of the claims  
9 requires “true security” against “high-value, strong attack situations.” MS Br., 28:9-17.

10          Microsoft fails, however, to adequately explain how the “context” of any particular claim  
11 requires the highest degree of security described in the patent specification. Claim 193.1, for  
12 example, involves downloading and playing music. This hardly seems the type of “high value,  
13 strong-attack” situation Microsoft describes. Microsoft gives no reason for assuming that the  
14 value and potential threats applicable to downloading songs is the same as the value and threats  
15 relevant, for example, to corporate trade secrets, nuclear weapons codes, money wire transfers,  
16 etc.

17           **4. Microsoft’s massive definition of “secure” invites the Court to usurp the**  
18           **jury’s role in conducting the infringement analysis.**

19          “Secure” is a general term, and the degree of protection necessary for a system to be  
20 “secure” depends on the context. The parties are in agreement on this, as is the specification.

21          When a claim term is drafted in general terms that may cover a range of circumstances,  
22 the Federal Circuit mandates that the Court construe the term generally and leave the question of  
23 determining whether an accused product meets that general construction to the finder of fact:

24           Claims are often drafted using terminology that is not as precise or specific as it  
25 might be. . . . That does not mean, however, that a court, under the rubric of  
26 claim construction, may give a claim whatever additional precision or specificity  
27 is necessary to facilitate a comparison between the claim and the accused product.  
Rather, after the court has defined the claim with whatever specificity and  
precision is warranted by the language of the claim and the evidence bearing on  
the proper construction, the task of determining whether the construed claim reads

28          <sup>1</sup> InterTrust agrees that the claims do not exclude the “true security” embodiment. That claims  
do not exclude an embodiment obviously does not mean the claims require that embodiment.

1 on the accused product is for the finder of fact.

2 The proper allocation of the tasks of construing a claim and determining  
3 infringement in a case in which a claim contains an imprecise limitation is  
4 demonstrated by our decision in Modine Mfg. Co. v. United States Int'l Trade  
5 Comm., 75 F.3d 1545, 37 U.S.P.Q.2D (BNA) 1609 (Fed. Cir. 1996). In Modine,  
6 the patentee had claimed a condenser for an automotive air conditioning system  
7 with "relatively small" hydraulic diameters. Id. at 1549. From the specification  
8 and prosecution history of the patent, this court concluded that the term "relatively  
9 small" should be interpreted as referring to a range of diameters of "about 0.015-  
10 0.040" inches. Id. at 1554. Instead of attempting to define that range more  
11 precisely, we remanded the case for a factual determination of whether the claim  
12 limitation was literally infringed by accused products having diameters ranging  
13 from 0.0424 to 0.0682 inch. Id. at 1554-55.

14 [T]he '886 patent contains some inherent imprecision resulting from the use of the  
15 term "consisting essentially of." As PPG points out, it is possible that under such  
16 circumstances different finders of fact could reach different conclusions regarding  
17 whether the effect of a particular unlisted ingredient in an accused product is  
18 material, and thus whether that product infringes. That possibility, however, is a  
19 necessary consequence of treating infringement as a question of fact subject to  
20 deferential review. It does not mean that the claim was improperly construed as an  
21 initial matter.

22 PPG Indus., Inc. v. Guardian Indus. Corp., 156 F.3d 1351, 1355 (Fed. Cir. 1998) (citation  
23 omitted).

24 PPG Industries is controlling here. "Secure" is a general term, the applicability of which  
25 depends on the context. The parties agree on this, and the patents describe different levels of  
26 security. The Court should, therefore, construe the term generally, and allow the jury to  
27 determine whether, under the particular circumstances, an accused product is or is not "secure."

28 **B. Microsoft's VDE-Based Interpretation Requires Excluding Disclosed Embodiments.**

The Federal Circuit is clear on constructions that exclude disclosed embodiments:

A claim construction that does not encompass a disclosed embodiment is thus  
"rarely, if ever, correct and would require highly persuasive evidentiary support."  
Vitronics, 90 F.3d at 1583, 39 U.S.P.Q.2D (BNA) at 1578.

Johns Hopkins Univ. v. CellPro, Inc., 152 F.3d 1342, 1355 (Fed. Cir. 1998) (emphasis added).

Microsoft's VDE-based constructions lead to exactly this result.

**1. Tamper-Resistant Barrier.**

Microsoft argues that "tamper resistant barrier" must be interpreted as a hardware device.  
MS Br., 30:22-23. As Microsoft acknowledges, however, "the Big Book also refers to a 'tamper

1 resistant barrier' which is not a physical hardware device." MS Br., 32:13-14.<sup>2</sup> In fact, the  
2 patent discusses this software embodiment at length, using the phrase "tamper resistant barrier"  
3 to refer to it. JCCS Ex. C, 22(B). Microsoft would thus have the Court construe "tamper  
4 resistant barrier" to exclude an embodiment identified in the specification as a "tamper resistant  
5 barrier." Why? Because defining "tamper resistant barrier" to include the software embodiment  
6 is inconsistent with VDE requirements Microsoft seeks to read into all of the claims (e.g., "true  
7 security," hardware Secure Processing Unit"). MS Br., 32:13-34:4.<sup>3</sup>

8 Microsoft's VDE construction is inconsistent with interpreting "tamper resistant barrier"  
9 to include the software "tamper resistant barrier." The Court therefore has a choice: accept  
10 Microsoft's VDE argument and construe this term in a manner contradicting the specification, or  
11 reject Microsoft's VDE construction and construe the term as it is used in the specification. As  
12 the Federal Circuit has held, the former of these approaches is "rarely, if ever" correct.

13 Moreover, InterTrust is aware of no Federal Circuit case that has ever held that a claim  
14 term can be interpreted to exclude, not merely a disclosed embodiment, but a disclosed  
15 embodiment that is identified in the specification using exactly the same words as the claim  
16 ("tamper resistant barrier"). Yet this is the result mandated by Microsoft's VDE construction.<sup>4</sup>

## 17 2. Protected processing environment.

18 Microsoft acknowledges that the specification discloses two embodiments of a protected  
19 processing environment, a hardware-based SPE and a software-based HPE, both of which are

20  
21 <sup>2</sup> Microsoft also alleges that the "ordinary meaning" of tamper resistant barrier connotes a  
22 physical device (MS Br., 30:24-28), but neither of its experts testifies to this effect, and  
23 Microsoft's only support is a misleading citation to Dr. Reiter, testimony that Dr. Reiter  
24 explicitly characterized as "an example." Reiter I, 137:22. (Keefe Decl., Ex. E.)

25 <sup>3</sup> Microsoft also alleges in a conclusory manner that a software tamper resistant barrier would be  
26 too vague since "there would be no objective measure for distinguishing between a barrier which  
27 is tamper resistant and one which is not tamper resistant" (MS Br., 32:7-9), but fails to discuss  
28 the lengthy specification disclosure discussing the software tamper resistant barrier (JCCS Ex. C,  
22(B)), nor does Microsoft address why a tamper resistant barrier provided by software requires  
an "objective measure" whereas no such objective measure is required for a hardware barrier.

<sup>4</sup> Moreover, the claim itself is inconsistent with Microsoft's interpretation. 721.1 recites not one  
but two tamper resistant barriers, and further recites that they have different security levels. The  
claim therefore clearly contemplates the possibility that one tamper resistant barrier will be more  
secure than another. For example, in one obvious embodiment, the first tamper resistant barrier  
would be hardware (higher security) and the second would be software (lower security).

1 explicitly identified as “protected processing environments.” MS Br., 34:3-14. As Microsoft  
2 further acknowledges, Microsoft’s definition of “protected processing environment” excludes the  
3 software-based HPE embodiment. MS Br., 35:3-14.

4 According to Microsoft, this is mandated for the same reason as exclusion of the software  
5 “tamper resistant barrier” from the construction of that term. MS Br., 35:12-14. Again,  
6 Microsoft’s VDE-based construction requires excluding a disclosed embodiment from the  
7 definition of a claim term, even though that embodiment is explicitly identified in the  
8 specification using the exact same term, and even though the specification explicitly states that  
9 “any service” may be provided by a secure HPE. ‘193 Patent, 80:35-36 (JCCS Ex. C, 22(B)).

10 Interpretation of claim terms so as to exclude embodiments distinctly described in the  
11 specification is clear legal error, yet this is precisely the result of Microsoft’s VDE-centric  
12 position.

13 **C. Microsoft’s Legal Arguments Are Misleading.**

14 Microsoft’s General Claim Construction Legal Analysis cites sources for the proposition  
15 that claims must recite the invention described in the specification. MS Br., 9:14-26. Microsoft  
16 emphasizes the word “invention” in these quotations, apparently hoping the Court will conclude  
17 that these cases and statutes stand for the proposition that, when the specification uses the word  
18 “invention,” every element described thereafter must be read into every claim.

19 In fact, none of the cited authority supports this proposition. That claims must recite the  
20 invention described in the specification does not mean that when a patent specification uses the  
21 word “invention,” the specification is automatically imported into the claims. InterTrust cited  
22 numerous Federal Circuit cases in its opening brief holding that elements described as the  
23 “invention” should not be read into the claims. InterTrust’s Opening Br., 9:1-10:24. Microsoft  
24 does not even attempt to distinguish this authority.

25 **D. Microsoft’s Argument that the Claims Require VDE is Wrong.**

26 **1. ‘193 patent claims.**

27 The ‘193 patent’s claims do not refer to “VDE,” nor to any other coined terms, such as  
28 “protected processing environment” or “host processing environment.” In its attempt to

1 shoehorn VDE into these claims, despite the absence of any VDE language, Microsoft relies on a  
2 variety of arguments that it repeats with respect to the other claims. First, Microsoft argues that  
3 the claims require elements that are not present in the claims themselves:

4 All four '193 Patent mini-Markman claims concern the distribution  
5 and protection of digital content, and contemplate multiple nodes  
6 and participants. Information is received (**possibly** from multiple  
7 upstream content providers), then stored on a device having  
8 **unspecified** authorized and unauthorized users, and then  
9 conditionally transferred to another device having **unspecified**  
10 users.

11 MS Br., 16:22-26 (emphasis added).

12 Why are the multiple content providers and multiple users “possible” and “unspecified?”  
13 Because the claims do not require them. The claims do not refer to multiple upstream content  
14 providers. The claims do not refer to multiple users of the first device, much less authorized and  
15 unauthorized users. The claims do not refer to multiple users of the second device.

16 The InterTrust claims are silent on these questions. The claims are consistent with  
17 multiple upstream content providers, but do not require them. The claims are consistent with  
18 multiple users of the first device, but do not require them. The claims are consistent with  
19 multiple users of the second device, but do not require them.

20 That claims are consistent with a particular embodiment is hardly grounds for reading  
21 every limitation from that embodiment into the claims.

22 Prof. Maier’s Declaration includes testimony that is apparently intended to buttress  
23 Microsoft’s argument. That testimony is worth quoting in full:

24 Additional **compelling evidence** of the presence of the Virtual Distribution  
25 Environment can be found in the process described in the claims themselves. For  
26 example, '193 Patent claim 1 purports to describes a distribution process  
27 involving at least three nodes. Thus, “receiving a digital file” implies, although  
28 does not explicitly state, that the digital file must come from some source device  
or system regardless of the transmission mechanism. Logically, this would be a  
system other than the “first device” and the “second device” which are described  
in other steps of the claim. Otherwise, the claim would have questionable utility.

Maier Decl., 23:17-25 (emphasis added).

This is typical of Microsoft’s Markman positions in general. Prof. Maier establishes that  
a “received” digital file must come from somewhere (a point not disputed by InterTrust), but

1 fails to explain why this is "compelling evidence" that the claims require VDE. Calling  
2 something "compelling evidence" does not make it so.

3 Microsoft's argument proceeds as follows:

4 This claim language (e.g., "if . . . allows," "determining whether") is not  
5 qualified. It implies that if the copying and storing are not allowed, then they are  
6 prevented (see Reiter Depo. at 174:1-178:11), no matter what effort may be made  
7 to take the unauthorized action. In other words, these claims imply that their  
8 "controls" are effective in the face of the attacks identified in the Big Book.

9 These claimed protections against misuse cannot be achieved by encrypting the  
10 content. Encryption would not prevent the content from being accessed, copied,  
11 distributed, or stored. For these types of protection, "access control" is necessary.  
12 More particularly, the Big Book describes only the complete "invention" as  
13 providing such protection against the threats identified in the Big Book. In other  
14 words, by promising the type of effective access control protection said to be  
15 provided only by the complete VDE, these claims invoke that "invention."

16 MS Br., 17:4-14.

17 This passage is typical of Microsoft's reasoning. First, it is almost entirely devoid of  
18 evidentiary citations. The only citation that Microsoft makes is to four pages of Dr. Reiter's  
19 deposition testimony, testimony that Microsoft has not even put into evidence (it is excluded  
20 from the Keefe Decl.). Microsoft's failure to provide this testimony to the Court is  
21 understandable, since Microsoft has grossly mischaracterized the passage, in which Dr. Reiter  
22 explicitly disclaimed any requirement of absolute protection. Reiter II, 177:18-178:11.  
23 Declaration of Jeff McDow in Support of InterTrust's Claim Construction ("McDow Decl."), ¶ 2  
24 and Ex. A.

25 Moreover, this passage is typical of Microsoft's arguments, since it piles inference on  
26 inference, none of them supported in any manner. Microsoft's chain of reasoning is as follows:

27 (1) The claims use the words "allows" and "determining," and do not qualify them.

28 (2) The absence of qualification means that the protections must be effective "no  
matter what effort may be made to take the unauthorized action." Microsoft makes this

allegation, but does not even allege that one of ordinary skill in the art would have understood  
the apparently innocuous terms "allows" and "determining" to require absolute protection.

(3) The requirement of absolute protection means that the controls must be "effective  
in the face of the attacks identified in the Big Book." Microsoft makes no allegation that every

1 attack described in the patent specification is relevant to these particular claims (e.g., music  
2 downloading), nor does it explain why every possible attack must be protected against.

3 (4) The requirement of absolute protection against all types of attacks “cannot be  
4 achieved by encrypting the content. Encryption would not prevent the content from being  
5 accessed, copied, distributed or stored.” Again, Microsoft presents no evidence for this  
6 proposition. Why, for example, would encryption not prevent content from being “accessed?”  
7 Microsoft doesn’t say. Moreover, the claims themselves don’t say anything about either the  
8 presence or the absence of encryption, and InterTrust has never alleged that the claims require  
9 encryption (nor that they exclude encryption for that matter).

10 (5) Since encryption is not sufficient, “[f]or these types of protection, ‘access control’  
11 is necessary.” The claims do not mention “access control.” No Microsoft witness testifies that  
12 one of ordinary skill in the art would have understood these claims as requiring “access control.”  
13 Instead, Microsoft imports “access control” into the claims because “access control” is allegedly  
14 better than encryption (also not mentioned in the claims) at ensuring the absolute degree of  
15 protection (also not mentioned in the claims) allegedly required by “allows” and “determining.”

16 (6) Since access control is required, the claims invoke VDE:

17 Microsoft’s argument reaches its conclusion in the following passage:

18 More particularly, the Big Book describes only the complete “invention” as  
19 providing such protection against the threats identified in the Big Book. In other  
20 words, by promising the type of effective access control protection said to be  
provided only by the complete VDE, these claims invoke that “invention.”

21 MS Br., 17:11-14.

22 This is a masterpiece of conclusory reasoning. “Such protection” is not mentioned in the  
23 claims, but is implied by Microsoft. The “threats identified in the Big Book” are not mentioned  
24 in the claims, but are implied by Microsoft. The claims do not make any type of “promise.”  
25 This is implied by Microsoft. The claims do not mention “access control,” either “effective” or  
26 non-effective. This is implied by Microsoft.

27 All of this, it should be recalled, rests on a rather thin reed: the presence of the words  
28 “allows” and “determining,” in the claims, yet Microsoft provides no basis for concluding that



1 one of ordinary skill would have interpreted these terms as implying hundreds of VDE  
2 limitations.

3 **2. '683, claim 2.**

4 Microsoft's justification for concluding that 683.2 should be interpreted as requiring the  
5 "hundreds" of VDE limitations is the following

6 This claim [683.2] also concerns a multi-node distribution system. Here, "secure  
7 containers" and "secure container rules" are distributed amongst various nodes.  
8 The claim appears to promise the ability to prevent access to or use of protected  
9 information, using the secure containers, secure container rules, and a "protected  
10 processing environment." (See Second Mitchell Decl. at 6-7). These protections  
11 are not qualified as to the nature or severity of the threat being faced; they  
12 impliedly are effective against all threats identified in the patent or Big Book.  
13 The only system described in the Big Book or '683 Patent said to accomplish such  
14 protections, is the complete VDE. This claim further invokes VDE by using VDE  
15 and vague terminology, such as "secure container" and "protected processing  
16 environment."

17 MS Br. 17:27-18:1.

18 The only support cited by Microsoft for this characterization of 683.2 is the Second  
19 Mitchell Decl. at 6-7. Those Declaration pages do not discuss this claim.

20 Microsoft's key argument is the following: "These protections are not qualified as to the  
21 nature or severity of the threat being faced; they impliedly are effective against all threats  
22 identified in the patent . . . ." Microsoft does not explain why an absence of qualification means  
23 the claims require the highest degree of security (as opposed to the lowest, or to the security  
24 relevant under the circumstances). Nor does Microsoft explain how this implication can be  
25 squared with specification statements that security may be limited, may be broken, or may  
26 consist of fewer than all protection mechanisms. JCCS Ex. C, 19(A)-(N), 19(Q)-(T).

27 **3. '721, Claims 1 and 34.**

28 Again, Microsoft's argument consists entirely of conclusory allegations. Microsoft  
argues that "The '721 Patent purports to improve the Big Book VDE by preventing the use of  
executable code (specifically "load modules" in Claim 1) except as authorized." MS Br., 18:8-9.  
No citation is given for this assertion, and Microsoft makes no attempt to tie it to the claims,  
other than noting that 721.1 recites load modules.

1 .. Microsoft continues by alleging that "Such prevention requires an access control  
2 capability." MS Br., 18:9-10. Again, no citation is provided, and neither claim mentions any  
3 such capability.

4 Microsoft then argues that the claims "promise such protections without any  
5 qualification." MS Br., 18:10-11. The claims contain no such promises, and Microsoft fails to  
6 explain why an absence of qualification requires the highest possible degree of protection.

7 Microsoft ends by arguing that the claims "invoke the 'invention'" by including the terms  
8 "protected processing environment," "tamper resistant barrier" and "security." As is discussed  
9 above, the first two of these are described using higher-security and lower-security embodiments,  
10 so these terms hardly support a requirement that the claims be interpreted using the highest  
11 possible security level. As to the word "security," this is a common word, and Microsoft  
12 provides no basis for reading a requirement of "VDE" into this term, other than the implication  
13 that VDE is the "context," an argument that is inconsistent with the multiple embodiments  
14 disclosed in the patents.

15 **4. Other claims.**

16 Microsoft's arguments regarding the other claims suffer from the same infirmities and  
17 should be rejected for the same reasons as discussed above.

18 **E. Microsoft's Bases for Reading the Specification Into the Claims Are Either**  
19 **Mischaracterized or Do Not Apply.**

20 Microsoft identifies various situations in which Microsoft believes that limitations can be  
21 read from the specification into the claims. MS Br. at 11:27-14:15. These situations are either  
22 mischaracterized by Microsoft or have no relevance to this case.

23 (1) To provide clarity. Microsoft cites cases for the proposition that, if a particular  
24 claim term deprives the claim of clarity, the court may look to the specification for guidance in  
25 interpreting the claim. MS Br., 11:27-12:13. Each of the cases cited by Microsoft concerned a  
26 particular interpretation issue raised by a particular claim element (e.g., does "automation code"  
27 mean particular code in an operating system? (Altiris, Inc. v. Symantec Corp., 318 F.3d 1363,  
28 1374-75 (Fed. Cir. 2003)); does "coupling" require different voltages? (NeoMagic Corp. v.

1 Trident Microsystems, Inc., 287 F.3d 1062, 1071-72 (Fed. Cir. 2002)); does “sealingly  
2 connected” require misaligned taper angles? (Watts v. XL Sys., Inc., 232 F.3d 877, 882-83 (Fed.  
3 Cir. 2000)); does “without significant cross-linking” include a particular type of cross-linking?  
4 (North Am. Vaccine v. American Cyanamid Co., 7 F.3d 1571, 1575-76 (Fed. Cir. 1993)).<sup>5</sup>

5 None of these cases involved an attempt by a patent defendant to read hundreds of  
6 limitations into every claim, nor to interpret numbers of claim terms using significant limitations  
7 that are not tied to any use of the terms themselves in the specification.

8 (2) Express or implied definition in the patent. Most of the cases cited by Microsoft  
9 involve an explicit definition in the patent or file history. Notably, where such definitions have  
10 been provided in the present case, Microsoft has chosen to ignore them (e.g., Device Class,  
11 Contained).

12 As Microsoft points out, the cases involving an “implied” definition concerned use of a  
13 claim term “throughout the entire patent specification in a manner consistent with only a single  
14 meaning.” MS Br., 12:19-20. In this case, however, Microsoft makes no attempt to establish  
15 that any particular claim terms are used consistently with only one meaning. Indeed, Microsoft  
16 regularly notes that the specification uses claim terms in multiple manners, or in a manner  
17 inconsistent with Microsoft’s proposed interpretation (e.g., “tamper resistant barrier,” “protected  
18 processing environment”).

19 (3) Important to the Invention. This issue is addressed in InterTrust’s opening brief.  
20 That specification characterizations of “the invention” do not constitute a magic formula  
21 automatically pulling the specification into the claims, however, is made clear by the cases cited  
22 in InterTrust’s opening brief, each involving specification statements about “the invention,” each  
23 holding that those statements did not limit the claims. Microsoft does not even attempt to  
24 distinguish these cases.

25 Microsoft’s characterization of SciMed Life Sys. v. Advanced Cardiovascular Sys., 242  
26 F.3d 1337 (Fed. Cir. 2001) is at best disingenuous: “limiting claim term ‘lumen’ to ‘coaxial

27  
28 <sup>5</sup> One of the cases cited by Microsoft (Ethicon Endo-Surgery v. United States Surgical Corp., 93  
F.3d 1572 (Fed. Cir. 1996)) is miscited, since the Federal Circuit used the prosecution history,

1 lumen' in part because the specification characterized the coaxial configuration as part of the  
2 'present invention.'" MS Br., 13:7-9. In fact, as InterTrust pointed out in its opening brief, the  
3 Scimed patent went well beyond characterizing this element as "part of" the invention: the  
4 specification stated that the element was present in "all embodiments" of the invention, a  
5 statement the Federal Circuit characterized as "the most compelling portion of the specification,"  
6 a statement that significantly exceeds anything present in the current case. 242 F.3d at 1343.

7 In addition, the cases cited by Microsoft involved specific issues relating to specific terms  
8 (Scimed: does "lumen" mean "coaxial lumen?"; Toro Co. v. White Consol. Indus., 199 F.3d  
9 1295, 1300-01 (Fed. Cir. 1999): does "including" mean "attached?"). Neither case held that  
10 statements about the "invention" required that an entire embodiment with hundreds of limitations  
11 be incorporated wholesale into every claim.

12 (4) Distinguishing prior art. Microsoft argues that statements distinguishing prior art  
13 may support reading embodiments into the claims. MS Br., 13:10-20. Cases cited by Microsoft  
14 generally concern file wrapper estoppel, Spectrum Int'l v. Sterilite Corp., 164 F.3d 1372, 1378  
15 (Fed. Cir. 1998); Rheox, Inc. v. Entact, Inc., 276 F.3d 1319, 1325-26 (Fed. Cir. 2002).<sup>6</sup>

16 The one case cited by Microsoft that does relate to a specification statement illustrates  
17 why this doctrine does not apply in the present case. In Innovad, Inc. v. Microsoft, 260 F.3d  
18 1326 (Fed. Cir. 2001), the court construed the claim term "dialer" in light of a specification  
19 statement that prior art dialers of a particular type were "useless" for a particular purpose. On  
20 that basis, the court concluded that the claim term "dialer" should exclude that particular type.

21 Here, in contrast, Microsoft points to no specification statement discussing a specific  
22 claim term in light of the prior art. For example, there are no specification statements to the  
23 effect that prior art software tamper resistant barriers were inadequate for some particular  
24 purpose. Nor does Microsoft cite any case standing for the proposition that a general statement  
25 about the inadequacies of the prior art and the advantages of an overall embodiment described in

26 rather than the specification, to interpret the claim element. 93 F.3d at 1579-80.

27 <sup>6</sup> CCS Fitness, Inc. v. Brunswick Corp., 288 F.3d 1359, 1366-67 (Fed. Cir. 2002) includes this  
28 factor in a list of possible factors but does not apply it, though it does cite the Spectrum file  
wrapper language.

1 the patent requires that every detail of that embodiment be read into every claim. Nor does Prof.  
2 Mitchell's testimony about various references fill this gap, since he does not tie his discussion of  
3 these references to any particular specification statement that distinguishes them. Mitchell 2nd  
4 Decl., 10:17-18:4.

5 (5) Express disclaimer. Microsoft does not argue that any express disclaimer exists.

6 **F. Microsoft's Argument about the InterTrust Divisionals Misses the Point.**

7 In its opening brief, InterTrust pointed out that the Patent Office's restriction requirement  
8 demonstrated that the foundational InterTrust application involved multiple inventions,  
9 inventions that the Patent Office expressly held related to separate classes, each shown to be  
10 "separately usable." InterTrust Opening Br., 11:5-12:20. This determination rebuts any  
11 argument that the original InterTrust specification disclosed only a single VDE "invention."

12 Microsoft makes arguments in response, but none to the point. Microsoft argues that the  
13 Patent Office's restriction requirement is irrelevant because "InterTrust's patent claims are free  
14 to recite additional features, which additional limitations may (or may not) make them separate  
15 'inventions' under Patent Office restriction practice. But, that is not the issue here." MS Br.,  
16 15:3-7.

17 Microsoft does not explain why "that is not the issue here," and it certainly seems to be  
18 the issue: Microsoft argues that the patents disclose a single, unitary VDE invention, and  
19 hundreds of limitations must be read into every claim. Microsoft relies heavily on statements  
20 referring to "the invention," and argues that "the invention" must be incorporated into every  
21 claim. The restriction requirement, however, makes it clear that references in the application to  
22 "the invention" cannot be read as meaning that the application recited a single invention.

23 Microsoft also points out that divisional patents may end up with claims directed to the  
24 same invention, and that in such a case the resulting patents are invalid. Microsoft further argues  
25 that, because the claims of the divisional applications were changed, the presumption they were  
26 directed to different inventions should not apply, citing Gerber Garment Tech., Inc. v. Lectra  
27 Sys. Inc., 916 F.2d 683 (Fed. Cir. 1990).

1        Gerber includes no such holding, nor could it, since the presumption of patent validity is  
2 statutory, and cannot disappear merely because a divisional application's claims have been  
3 changed. The Court must presume that the Patent Office acted properly in the original restriction  
4 requirement, and in issuing the subsequent patents, including the amended claims. Thus, the  
5 Court must presume that the divisional applications were originally drawn to different  
6 inventions, and that the subsequent patents issuing from those applications were also drawn to  
7 different inventions, since otherwise the divisional patents would be invalid, and those patents  
8 carry a statutory presumption of validity.

9        Microsoft characterizes Ballard Med. Prod. v. Allegiance Healthcare Corp., 268 F.3d  
10 1352 (Fed. Cir. 2001), as follows: "limiting claims of both a patent issued from the parent  
11 application and a patent issued from a divisional of such parent to exclude a particular type of  
12 valve based on statements made in common specification text and prosecution history of the  
13 parent application." MS Br., 15:26-16:2. This is wrong. In Ballard, the Federal Circuit held that  
14 statements in a parent prosecution history can serve to limit later patents. 268 F.3d at 1361-62.  
15 No issue of statements made in the specification was raised in the case. In particular, the Federal  
16 Circuit did not address specification statements about "the invention."<sup>7</sup>

17 **G. Individual Claim Elements.**

18 **1. Microsoft ignores ten claim elements.**

19        Microsoft filed a forty page brief, plus two expert Declarations, but neither Microsoft nor  
20 its experts have anything to say about ten of the thirty terms at issue in this hearing: (1) Aspect,  
21 (2) Authentication, (3) Compares, (4) Derive, (5) Designating, (6) Device Class, (7) Digital  
22 Signature/Digitally Signing, (8) Executable Programming/Executable, (9) 721.1: "digitally  
23 signing a second load module...." (10) 912.8: "identifying at least one aspect of an execution  
24 space required for use and/or execution of the load module."

25  
26  
27 <sup>7</sup> Moreover, Ballard involved claims interpreted under 35 U.S.C. § 112(6), which are supposed to  
28 be limited to the embodiments disclosed in the specification, so this case would be  
distinguishable even if Microsoft had correctly characterized it. 283 F.3d at 1359-60.

1           2.     Use.

2           InterTrust's definition is taken from a standard dictionary (JCCS, Ex. C, 23(A)). The  
3 Federal Circuit approves using dictionary definitions. Inverness Med. Switz. GmbH v. Princeton  
4 Biomeditech Corp., 309 F.3d 1365, 1369-70 (Fed. Cir. 2002).

5           Microsoft's argument on "use" is mysterious, as Microsoft concentrates on "encryption,"  
6 and on a series of alleged InterTrust contentions. MS Br., 20:6, 21:20-25. Encryption appears  
7 irrelevant to the proposed definitions, and InterTrust never made the contentions.

8           3.     Copy.

9           Microsoft responds at length to arguments never made by InterTrust, and ignores  
10 InterTrust's central point: Microsoft's definition would result in a nonsensical interpretation of  
11 193.1, in which a budget for making copies would be used up by "phantom," internal  
12 reproductions that the user would never know existed, much less be able to use. Microsoft does  
13 not attempt to explain how its interpretation would make sense in the context of the claim.<sup>8</sup>

14          4.     Secure/Securely.

15          Microsoft acknowledges that its proposed definition is neither "standard" nor an express  
16 definition from the patent. MS Br. at 28:6-7. What Microsoft fails to acknowledge is that its  
17 definition actually contradicts the specification. According to Microsoft, a system is secure only  
18 if it protects five separate properties against attack, and only if this protection is 100% effective.  
19 As described above (§ II A 2), however, the specification explicitly describes various levels of  
20 security, and characterizes them all as "secure."

21          Microsoft attacks InterTrust's definition, arguing that InterTrust ignores the effectiveness  
22 of the efforts taken. MS Br., 26:10-11. In fact, InterTrust's proposed definition requires that the  
23 mechanisms employed "prevent," "detect" or "discourage" misuse or interference. A  
24 mechanism that fails to perform these functions (e.g., a completely ineffective mechanism)  
25 would not be "secure" under InterTrust's definition.

26  
27 <sup>8</sup> Prof. Mitchell's commentary on "copy" is similar: a great deal of discussion of this phrase in  
28 the abstract, but no attempt to explain how Microsoft's proposed definition would make sense in  
the context of the claim, nor any attempt to respond to InterTrust's discussion of this in its  
opening Brief. Mitchell 2nd Decl., 6:23-8:2.

1 Microsoft also argues that VDE "promises the ability to prevent" various types of misuse,  
2 and that detecting or discouraging misuse is not security. MS Br. at 26:14-20. Microsoft cites  
3 no support for this proposition, and it is clearly incorrect. In some circumstances, mechanisms  
4 that allow the detection of misuse are fully sufficient for security. For example, technology that  
5 made it possible to detect an alteration of a driver's license would render the driver's license  
6 "secure," since, although the driver's license could be altered (e.g., to change the birthdate of an  
7 underage would-be drinker), the fact that the change could be detected would make it impossible  
8 for an attacker to gain any benefit from the misuse.

9 Thus, one disclosed embodiment of the tamper-resistant barrier "detects tampering and/or  
10 destroys sensitive information." JCCS Ex. C, 22(A). It is impossible to read this passage of the  
11 specification as requiring any protection mechanism other than "detection."

12 Microsoft also mischaracterizes Dr. Reiter's testimony, alleging he testified that none of  
13 the five listed forms of protection is required. MS Br., 27:1-3. As with so many of Microsoft's  
14 citations, however, this one is false. In the cited passage from Dr. Reiter's deposition, a  
15 Microsoft attorney asked a series of questions, each question relating to a single mechanism.  
16 Since security requires one or more of these mechanisms, but does not require all of them, Dr.  
17 Reiter correctly answered "no" when asked whether the claims required each mechanism in  
18 isolation. Dr. Reiter was never asked whether at least one mechanism from the entire group was  
19 required, and he never testified that security could exist without any mechanism at all. Reiter  
20 202:5-204:14 (McDow Decl., Ex. A.)<sup>9</sup>

#### 21 5. Secure Container.

22 Microsoft alleges that only a single embodiment is disclosed, and that it requires the  
23 ACCESS method. MS Br., 29:10-13. This is false. The ACCESS method excerpts quoted by  
24 Microsoft are part of a longer passage that is expressly described as being an "an example" ('193  
25 patent, 192:2), and the same passage describes the ACCESS method Microsoft cites as a

26  
27 <sup>9</sup> Similarly, suppose a movie theater offered half-price tickets to customers ages ten to twelve,  
28 and a particularly obtuse customer posed the following series of questions: "Do I have to be 10  
to receive the discount?" "Do I have to be 11 to receive the discount?" "Do I have to be 12 to  
receive the discount?" The answer to all three questions would be "no," but this obviously



1 "complicated procedure" and notes that "in many cases" a "relatively trivial" procedure may be  
2 used instead. Id. at 192:6-11.

3 In addition, Microsoft argues that the "access control ability of VDE secure containers" is  
4 "critical to VDE's promise to content owners." MS Br., 28:3-7. The phrase "VDE secure  
5 container" does not appear in the '193 patent. McDow Decl., ¶ 3. When the inventors wanted to  
6 refer to a container in terms of VDE capabilities, they explicitly identified it as a "VDE  
7 container" (e.g., JCCS Ex. C, 20(E)). The patent claims do not refer to "VDE containers," but  
8 instead refer to "secure containers."<sup>10</sup> Microsoft seeks to confuse this issue by using the phrase  
9 "VDE secure containers," in an apparent attempt to mislead the Court into believing that "secure  
10 containers" and "VDE containers" are identical.<sup>11</sup>

11 **6. Tamper Resistant Barrier.**

12 As discussed above, Microsoft's construction of "tamper resistant barrier" admittedly  
13 excludes an embodiment that is referred to in the specification as a "tamper resistant barrier."  
14 Microsoft's argument also suffers from other defects. Microsoft alleges that the specification  
15 requires a hardware barrier wherever content is "assigned usage control information, or used."  
16 MS Br. at 33:10-14. Microsoft quotes several excerpts at length, none of which even mentions  
17 tamper resistant barriers, much less excludes software tamper resistant barriers.

18 Moreover, the term "tamper resistant barrier" is recited only in 721.34. Microsoft rather  
19 casually alleges that "all of the mini-Markman claims contemplate one or both of these two  
20 conditions" (i.e., assigning usage control information to content or using content). MS Br.,  
21 33:10-12. Claim 721.34 has no reference to assigning usage control information or any use of  
22 content, nor does it have any language from which such elements can be inferred.

23  
24 wouldn't establish that the discount is an illusion.

25 <sup>10</sup> InterTrust agrees that "VDE containers" are one embodiment of "secure container," but this  
26 obviously does not mean that all "secure containers" are "VDE containers."

27 <sup>11</sup> Prof. Maier states that "I believe it is apparent that [secure container] is intended to refer to the  
28 VDE container." Maier Decl., 22:17-18. He gives no basis for this belief, nor does he explain  
how "secure container" is used in the specification, other than noting it only occurs twice in the  
'193 patent. This statement is itself misleading, since it ignores the extensive use of the term in  
the '683 and '861 patents, both of which include mini-Markman claims using "secure container."  
McDow Decl., ¶ 5.

1 In addition, Microsoft's argument that a hardware barrier is required ignores alternative  
2 embodiments described in the specification. For example, Microsoft ignores the excerpt cited by  
3 InterTrust at JCCS Ex. C, 22(B), which describes a "secure HPE" with a software tamper  
4 resistant barrier, and states that "Any service may be provided by such a secure HPE . . . ."

5 Prof. Maier alleges that the "tamper resistant barrier" recited in the claims is referred to  
6 as a "tamper resistant security barrier," or a "tamper-resistant hardware security barrier." Maier  
7 Decl. 34:21-23. The claim uses the term "tamper resistant barrier," rather than these other  
8 phrases. That the specification uses these other phrases to refer to hardware barriers is evidence  
9 that the unqualified phrase "tamper resistant barrier" should apply to both embodiments.

10 Prof. Maier acknowledges that the patent "alludes to" a software tamper resistant barrier,  
11 but he states that "the specification gives no indication how to determine what the boundaries of  
12 such a 'barrier' might be or how to implement such techniques successfully." Maier Decl., 35:7-  
13 10. The quotation (JCCS Ex. C, 22(B)) contains more than an "allusion" to a software tamper  
14 resistant barrier, it explicitly describes numerous techniques that may be used to provide one.

#### 15 **7. Protected Processing Environment.**

16 Microsoft's main argument regarding this term is discussed above in § II B 2, and its  
17 other arguments amount to quibbles that InterTrust's definition is not specific enough. No claim  
18 construction can address every possible infringement issue. As the Federal Circuit has held, if a  
19 claim term is reasonably defined in general terms, it is the Court's obligation to adopt that  
20 construction, leaving the question of application of the general definition to the jury. PPG  
21 Industries, 156 F.3d at 1354-55.

#### 22 **8. Component Assembly.**

23 Microsoft asserts that "In the Big Book the term 'component assembly' (also called  
24 'component') uniformly is used to refer to executable components, which are an assembly of  
25 independent, executable load modules and data." MS Br. at 35:12-14. Microsoft provides no  
26 support for the assertion that a "component assembly" is also called a "component," an assertion  
27 that seems odd, since a "component assembly" is self-evidently an assembly of components.

28

1 Microsoft's main argument is that InterTrust's definition would allow the possibility of a  
2 component assembly that does not include any executable code. InterTrust did not intend to  
3 leave open the possibility that a component assembly might include no programming. InterTrust  
4 is willing to amend the third sentence of its proposed construction to read as follows:  
5 "Component Assemblies must include code, and are utilized to perform operating system and/or  
6 applications tasks."

7 Microsoft makes no attempt to otherwise defend its complicated definition.

8 Prof. Maier's discussion of "component assembly" notes that the specification describes  
9 multiple embodiments (Maier Decl., 17:1-3), but appears to consider this to be an improper  
10 practice. At a later point in his Declaration, Prof. Maier states that InterTrust's citations relating  
11 to "component assembly" all relate to VDE, though he only quotes language from two of these  
12 citations. Maier Decl., 27:2-10. Prof. Maier appears not to have appreciated the point of a  
13 number of these quotations: that the VDE-related description of "component assembly" is  
14 expressly and repeatedly referred to as a "preferred embodiment."

15 **9. Control (noun).**

16 Microsoft's argument includes an analogy relating to librarians, but without any support  
17 from the experts or the patents that this analogy is reasonable or correct. Thus, Microsoft argues  
18 that "rules" and "controls" should not be equated, on the basis that "rules" are non-executable,  
19 whereas controls are "executable." Microsoft presents no evidence for its assertion that "rules"  
20 are non-executable, other than the argument that "rules" constitute the "guard" in Microsoft's  
21 analogy.

22 Moreover, the quotations cited by Microsoft in its brief and in JCCS Ex. D do not state  
23 that a "control" must be executable, but instead are merely consistent with "controls" being  
24 executable programming, as is InterTrust's proposed definition.

25 Prof. Maier argues that "control" should be interpreted in light of VDE because 75% of  
26 the passages cited by InterTrust allegedly relate to VDE. Maier Decl., 28:2-3. Prof. Maier does  
27 not explain the significance of this statistic, and it does not seem to have occurred to Prof. Maier  
28 that the non-VDE uses constitute evidence that the term should not be limited to VDE.

1           **10. A budget specifying the number of copies which can be made of said digital**  
2           **file (193.1).**

3           Microsoft argues that InterTrust's construction does not specify "since when," "by  
4           whom" or "by what." The claim does not require this information, and Microsoft does not  
5           explain why a budget must include it.

6           **11. Container.**

7           Although Microsoft discusses this word separately (MS Br., 39:3-7), "container" is not a  
8           disputed term, but instead occurs as part of "secure container." InterTrust's definition of "secure  
9           container" rests on a definition of "container" from the Microsoft Computer Dictionary and is  
10          consistent with use of the term in the mini-Markman patents, and a contemporaneous Microsoft  
11          patent. JCCS Ex. C, 20(I), (J).

12          Microsoft argues that, in the patents, "container" is not used in the manner asserted by  
13          InterTrust, citing Alexander Decl. 20(A)-(D). Microsoft provides no explanation for why these  
14          passages are inconsistent with InterTrust's construction.

15          **12. Containing.**

16          The patent explicitly defines "containing" as including referencing. JCCS Ex. C, 7(B).  
17          Microsoft's argument about the "ordinary meaning" of the term is both unsupported and  
18          irrelevant in light of this explicit definition, and in light of the Microsoft Computer Dictionary  
19          definition for "container" ("a file containing linked or embedded objects"). JCCS Ex. C, 20(I).

20          **13. Control (verb) / Controlling.**

21          InterTrust's definition comes directly from a standard dictionary. Microsoft's only  
22          response is that this is inconsistent with VDE. Microsoft fails, however, to cite any text from the  
23          patents defining "controlling" in any particular manner, and the only quotation it includes does  
24          not even use "control" as a verb. As InterTrust pointed out in its opening brief, the patents use  
25          "control" as a verb in many non-VDE contexts. InterTrust Opening Br., 21:23-28.

26          **14. "Controlling the copies made of said digital file" (193.1).**

27          Microsoft does not attempt to support its proposed definition, which is long and complex.  
28          Instead, Microsoft quibbles about implications arising from InterTrust's construction.

1 The InterTrust construction is based on the manner in which this phrase is used in the  
2 claim, in which it explains the “copy control.” See JCCS Ex. A, Row 7. The nature of the copy  
3 control is further described later in the claim. JCCS Ex. A, Rows 8 and 9. InterTrust’s definition  
4 is based on the phrase itself and on its context in the claim, a context Microsoft entirely ignores.

5 **15. “Derives information from one or more aspects of said host processing  
6 environment” (900.155).**

7 Microsoft’s argument consists of unsupported allegations, including the assertion that a  
8 “unique” signature is required, that “the derived information may serve no security purpose at  
9 all,” and that this “is contrary to the patent.” Microsoft’s Ex. D evidence for this term consists of  
10 122 separate citations amounting to twenty pages. Since Microsoft’s allegations are not tied to  
11 any particular text, InterTrust cannot respond, other than stating that any text Microsoft may  
12 subsequently identify will simply be an embodiment, since this term occurs frequently in the  
13 passages quoted in Microsoft’s JCCS Ex. D.<sup>12</sup>

14 **16. Host Processing Environment.**

15 In its opening brief, InterTrust acknowledged that its definition of Host Processing  
16 Environment does not include the “insecure” variant, and proposed an alternate definition.  
17 InterTrust Br., 36:13-19. Microsoft ignores this, criticizing InterTrust for failing to cover  
18 insecure host processing environments. MS Br., 40:10-13. Microsoft otherwise fails to respond  
19 to any of InterTrust’s points on Host Processing Environment. InterTrust Br., 36:20-37:10.

20 **17. Identifier.<sup>13</sup>**

21 Microsoft claims that InterTrust’s definition of “identify” is “contrary to the ordinary  
22 meaning.” InterTrust’s definition is from the American Heritage Dictionary. JCCS Ex. C, 17(F).

23 <sup>12</sup> If Microsoft subsequently identifies particular relevant passages, InterTrust will move to strike  
24 those identifications as being inconsistent with this Court’s Patent Local Rules. It is one thing to  
25 make assertions that are supported by one or two pages of quoted text. It’s quite another to make  
26 general arguments that are not supported by any individual citations but are instead allegedly  
27 supported by twenty pages of block quotes. The Patent Local Rules require the parties to  
28 identify relevant evidence. Twenty pages of unexplained quotes do not comply with this  
requirement.

<sup>13</sup> Microsoft’s brief discusses “identifying (identify),” neither of which are terms to be construed  
in this proceeding. MS Br., 40:14. Since Microsoft also cites the JCCS Ex. A reference  
covering “identifier,” InterTrust will assume that Microsoft is intending to discuss this term, and  
will respond accordingly.

1           **18. Tamper Resistance.**

2           Microsoft's argument consists of an unsupported assertion ("plainly is not what VDE  
3 means by 'tamper resistance'") and a quibble ("more than difficult [sic] than what?"). MS Br.,  
4 40:21-25. As to the former, assertions do not constitute evidence supporting Microsoft's  
5 construction. As to the latter, more difficult than if the tamper resistance were not present.

6           Prof. Maier, on the other hand, spends considerable time discussing this concept,  
7 including two pages of symbolic logic, apparently intended to prove that tamper resistance  
8 cannot include detection of tampering. Maier Decl., 32-34. However, whatever the details of  
9 Prof. Maier's analysis, he simply fails to address JCCS Ex. C 21(B), a quotation that explicitly  
10 states that a tamper resistant barrier "detects tampering and/or destroys sensitive information."  
11 This quotation clearly equates tamper resistance with detecting tampering, and does not require  
12 that tampering actually be blocked.

13           **19. Budget.**

14           Although Microsoft's brief does not refer to "budget," Prof. Maier's Declaration  
15 discusses this term, though without any citation to the claims or specification. Maier Decl., 17:6-  
16 13. Prof. Maier acknowledges that the specification sometimes uses "budget" to refer to data  
17 and in other places uses "budget" to refer to executables, but treats this as an "inconsistency" that  
18 leads to "confusion" (Maier Decl., 17:11) rather than as multiple embodiments that establish the  
19 term can refer to either data or an executable.

20           **20. Clearinghouse.**

21           Prof. Maier alleges that "clearinghouse" has "a specific meaning in the banking and  
22 commerce fields." Maier Decl., 24:1-2. Unfortunately, he fails to explain what this alleged  
23 meaning might be, or how it would support reading VDE features into the claims. Instead, he  
24 cites some quotations from InterTrust, but does not respond to a primary point made in  
25 InterTrust's opening brief: Visa and AT&T are identified in the specification as  
26 "clearinghouses," yet no one could believe that either Visa or AT&T have the various VDE  
27 features required by Microsoft's proposed definition.

28

1 H. Testimony Cited by Microsoft.

2 Exhibit A to the Keefe Declaration contains numerous quotations that Microsoft does not  
3 refer to in its brief. Most of these quotations are from inventors or third party deponents. The  
4 inventor testimony is not tied to the patents, and "The subjective intent of the inventor when he  
5 used a particular term is of little or no probative weight in determining the scope of a claim  
6 (except as documented in the prosecution history)." Markman v. Westview Instruments, Inc., 52  
7 F.3d 967, 985-86, aff'd, 517 U.S. 370 (1996). The third party testimony suffers from the same  
8 defects as the testimony InterTrust moved to strike in connection with Microsoft's summary  
9 judgment motion, and is incompetent for those same reasons.

10 III. CONCLUSION.

11 Microsoft's VDE-centric claim interpretation would require the Court to ignore  
12 embodiments disclosed in the specification, and to interpret particular claim terms in a manner  
13 that excludes disclosed embodiments, a practice the Federal Circuit has held is "rarely, if ever,"  
14 correct. Microsoft supports this extreme position with conclusory reasoning and egregious  
15 miscitations of the record.

16 Microsoft's claim constructions are longer and more complicated than any constructions  
17 ever adopted by any court. Those constructions would read literally hundreds of limitations into  
18 every single claim. InterTrust respectfully requests that the Court reject Microsoft's VDE-  
19 centric interpretation position and adopt the claim constructions proposed by InterTrust.

20 Dated: April 21, 2003

Respectfully submitted,

21 DERWIN & SIEGEL, LLP

22

23

24

25

26

27

28

By: 

DOUGLAS K. DERWIN  
Attorney for Plaintiff  
INTERTRUST TECHNOLOGIES  
CORPORATION